

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method comprising:

reading from a first software module a set of keys associated with a trusted source, wherein the set of keys is embedded in the first software module;
determining whether a key presented by or read from a second software module is traceable to one of the keys in the set of keys;
determining whether the key is identified in a list of compromised keys; and
if the key is not identified as compromised and is traceable to one of the keys in the set of keys, assigning the key a trusted status.

2. (Original) The method of claim 1 further comprising:

verifying the integrity of a document comprising the key and the list of compromised keys.

3. (Cancelled).

4. (Previously Presented) The method of claim 1 in which determining whether the key is traceable to one of the keys in the set of keys further comprises:

tracing the key through a certificate chain to one of the keys in the set of keys.

5. (Currently Amended) The method of claim 1 further comprising:

associating a document comprising the key and the set of keys with ~~a~~the first software module comprising the set of keys using a hash of the first software module in the document.

6. (Original) The method of claim 2 in which the document is a manifest signed by the key.

7. (Original) The method of claim 1 in which determining whether the key is identified in the list of compromised keys further comprises:

searching the list of compromised keys for the key.

8. (Currently Amended) A method comprising:

producing a document comprising an identification of a first software module and a list of compromised keys; and

digitally signing the document using a key presented by or read from a second software module and traceable to one key of a set of keys, wherein the set of keys is embedded in the first software module.

9. (Currently Amended) The method of claim 8 in which the identification of the first software module comprises a hash value of the first software module.

10. (Currently Amended) The method of claim 8 in which the key is traceable to one of the keys in the set of keys embedded in the first software module by way of a certificate chain.

11. (Currently Amended) The method of claim 8 further comprising:

making the document available on a communication network by which computer systems comprising the first software module may read the document.

12. (Cancelled).

13. (Currently Amended) A device comprising:

a processor;

a machine-readable storage medium coupled to the processor by way of a bus, the storage medium storing instructions which, when executed by the processor, cause

the device to determine whether a key presented by or accessed from a software module is traceable to one key of a set of keys associated with a trusted source;

determine whether the key is identified in a list of compromised keys; and
if the key is not identified as compromised and is traceable to one of the keys in the set of keys, assign the key a trusted status.

14. (Previously Presented) The device of claim 13 in which the instructions, when executed by the device, further cause the device to:

verify the integrity of a document comprising the key and the list of compromised keys.

15. (Currently Amended) The device of claim 13 further comprising another software module comprising the ~~list~~set of keys.

16. (Previously Presented) The device of claim 13 in which the instructions, when executed by the device, further cause the device to:

trace the key through a certificate chain to one of the keys in the set of keys.

17. (Currently Amended) A device comprising:

a processor;

a machine-readable storage medium coupled to the processor by way of a bus, the storage medium storing instructions which, when executed by the processor, cause the device to:

produce a document comprising an identification of a first software module and a list of compromised keys; and

digitally sign the document using a key presented by or read from a second software module and traceable to one key of a set of keys, wherein the set of keys is embedded in the first software module.

18. (Currently Amended) The device of claim 17 in which the identification of the first software module comprises a hash value of the first software module.

19. (Currently Amended) The device of claim 17 in which the key is traceable to one of the keys in the set of keys embedded in the first software module by way of a certificate chain.

20. (Currently Amended) An article comprising a machine-readable medium having stored thereon instructions which, when executed by a processor, result in:

reading from a first software module a set of keys associated with a trusted source, wherein the set of keys is embedded in the first software module;

determining whether a key presented by or read from a second software module is traceable to one of the keys in the set of keys;

determining whether the key is identified in a list of compromised keys; and

if the key is not identified as compromised and is traceable to one of keys in the set of keys, assigning the key a trusted status.

21. (Previously Presented) The article of claim 20 in which the instructions, when executed by the processor, further result in:

verifying the integrity of a document comprising the key and the list of compromised keys.

22. (Cancelled).

23. (Previously Presented) The article of claim 20 in which the sequence of instructions, when executed by the processor, further result in:

tracing the key through a certificate chain to one of the keys in the set of keys.

24. (Currently Amended) An article comprising a machine-readable medium having stored thereon instructions which, when executed by a processor, result in:

producing a document comprising an identification of a first software module and a list of compromised keys; and

digitally signing the document using a key presented by or read from a second software module and traceable to one key of a set of keys, wherein the set of keys is embedded in the first software module.

25. (Currently Amended) The article of claim 24 in which the identification of the first software module comprises a hash value of the first software module.

26. (Currently Amended) The article of claim 24 in which the key is traceable by way of a certificate chain to one of the keys in the set of keys embedded in the first software module.